FRI-2G.303-1-CCT1-06

TEACHING CRYPTOGRAPHY AND DATA SECURITY: SIMPLIFIED MD4 HASH FUNCTION[6]

Assist. Prof. Emilia Golemanova, PhD
Department of Computer Systems and Technologies,
"Angel Kanchev" University of Ruse
Tel.: 082-888-681
E-mail: EGolemanova@uni-ruse.bg

Assist. Prof. Tzanko Golemanov, PhD
Department of Computer Systems and Technologies,
"Angel Kanchev" University of Ruse
Tel.: 082-888-681
E-mail: TGolemanov@uni-ruse.bg

Abstract: *Cryptographic hash functions are data integrity algorithms used in a variety of security applications like message authentication, digital signatures, one-way password files, intrusion detection, and virus detection. Although the SHA algorithms (inspired by the MD family) are the most widely used hash functions nowadays, teaching the MDx algorithm first is an approach adopted in most Cryptography and Data Security courses. The paper describes the teaching process of MD4 at the department of Computer Systems and Technologies of Ruse University. MD4 algorithm lays the foundation for several other popular hash functions like MD5, SHA-1, SHA-2, and RIPEMD. Due to the large number of operations in the full MD4, a simplified version suitable for students to work with by hand in a classroom setting is used. The authors present an especially developed educational tool for better apprehending simplified MD4.*

Keywords: *Cryptography, Hash function, MD4, Teaching tool*

ВЪВЕДЕНИЕ

Криптографските хеш-функции са алгоритми, осигуряващи цялостност (интегритет) на данните. Вероятно те са едни от най-гъвкавите криптографски примитиви, използвани за различни цели:

- самостоятелно: като цифров отпечатък на файлове, публични ключове или пароли;
- комбинирани с криптиращи функции: за автентикация на съобщението (например MAC) или за по-ефективна реализация на концепцията за цифров подпис.

Затова преподаването им играе съществена роля във всеки курс по „Криптография и защита на данните".

Въпреки че SHA-алгоритмите, инспирирани от фамилията MD, са най-разпространените хеш-функции днес, изучаването първо на MD-алгоритъм е възприет подход в повечето курсове по криптография, тъй като осигурява разбиране на основните принципи, използвани в съвременните криптографски хеш-функции. MD4 (Network Working Group, 1990) стои в основата за няколко други популярни хеш-функции като MD5 (Network Working Group, 1992) , SHA-1 (National Institute of Standards and Technology, 1995), SHA-2 (National Institute of Standards and Technology, 2001) и RIPEMD (Bosselaers, 1995) (Dobbertin, 1996).

Докладът описва подхода при преподаването на MD4, използван в катедра „Компютърни системи и технологии" на Русенски университет. Поради големината на данните и многото операции в MD4, по време на практическите занятия по дисциплината се използва опростена версия (S-MD4), позволяваща на обучавания да извърши хеширане на ръка и да придобие детайлна представа за работата на алгоритъма. Макар и опростена версия на MD4,

[6] Докладът е представен на сесия на секция 3.2 на 28 октомври 2022 с оригинално заглавие на български език: ОБУЧЕНИЕ ПО КРИПТОГРАФИЯ И ЗАЩИТА НА ДАННИТЕ: ОПРОСТЕНА MD4 ХЕШ-ФУНКЦИЯ

преподаването на S-MD4 е предизвикателство и за обучаващия. Преподавателят се нуждае от удобен симулатор, чрез който да обясни алгоритъма за конкретен пример. Освен това добре е да разполага със софтуер, автоматизиращ процеса на самопроверка и тестване. За съжаление, повечето от използваните автоматизирани средства за обучение по S-MD4 са по-скоро калкулатори (Online hash calculation MD4 Algorithm, 2022) (Online MD4 Generator, 2022) (Online MD4 Hash Calculator, 2022), представящи само окончателния резултат от работата на алгоритъма, а не отделните стъпки.

Авторите представят специално разработения инструмент за целите на обучението и тестването на S-MD4.

ИЗЛОЖЕНИЕ

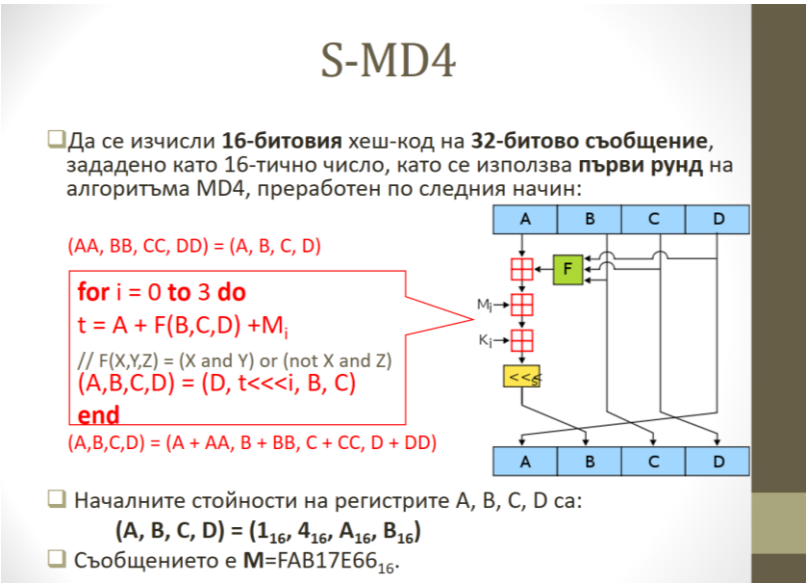
Опростен MD4 (S-MD4)

Опростената версия на MD4, използвана за учебни цели, има същата архитектура като тази на реалната криптографска функция, но се различава по следните параметри:

Таблица 1. Разлика между MD4 и S-MD4

Параметри	MD4	S-MD4
message block	512 bits = 16 words	16 bits = 4 hexadecimal digits
hash value	128 bits	16 bits = 4 hexadecimal digits
register	32 bits	4 bits = 1 hexadecimal digit
number of rounds	3	1 (the first one in MD4)
number of operations in one round	16	4
message block processed in one operation (M_i)	32 bits = 1 word	4 bits = 1 hexadecimal digit

Задачата, която студентите решават е представена на Фиг. 1:



Фиг. 1. Обща схема на S-DES

За решаването на тази задача студентите разполагат с инструментално средство, авторска разработка, което се използва както по време на практическите занятия, така и при самоподготовка. Освен това изборът на език (български, английски, руски) дава възможност за използването му за обучение и на чуждестранни студенти. Има три основни режима на работа:

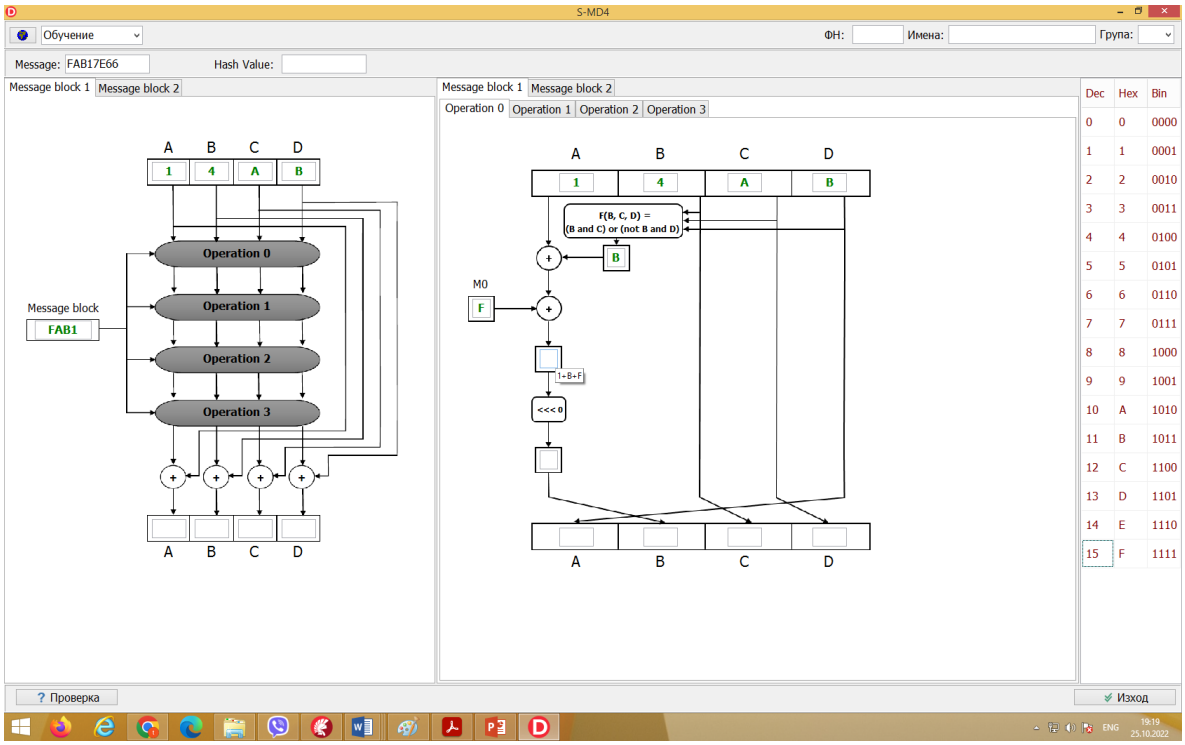
- режим „Обучение“;

- режим „Самообучение“;
- режим „Тест“.

Предложеният софтуерен продукт **S-MD4 Tool** е разработен чрез Embarcadero® Delphi в средата на Embarcadero RAD Studio 10.3.3 Rio и има интерфейс, представящ схематично алгоритъма, по подобие на (Holden, 2013), а не чрез псевдо-код, което подпомага разбирането на алгоритъма.

S-MD4 Tool: Обучение

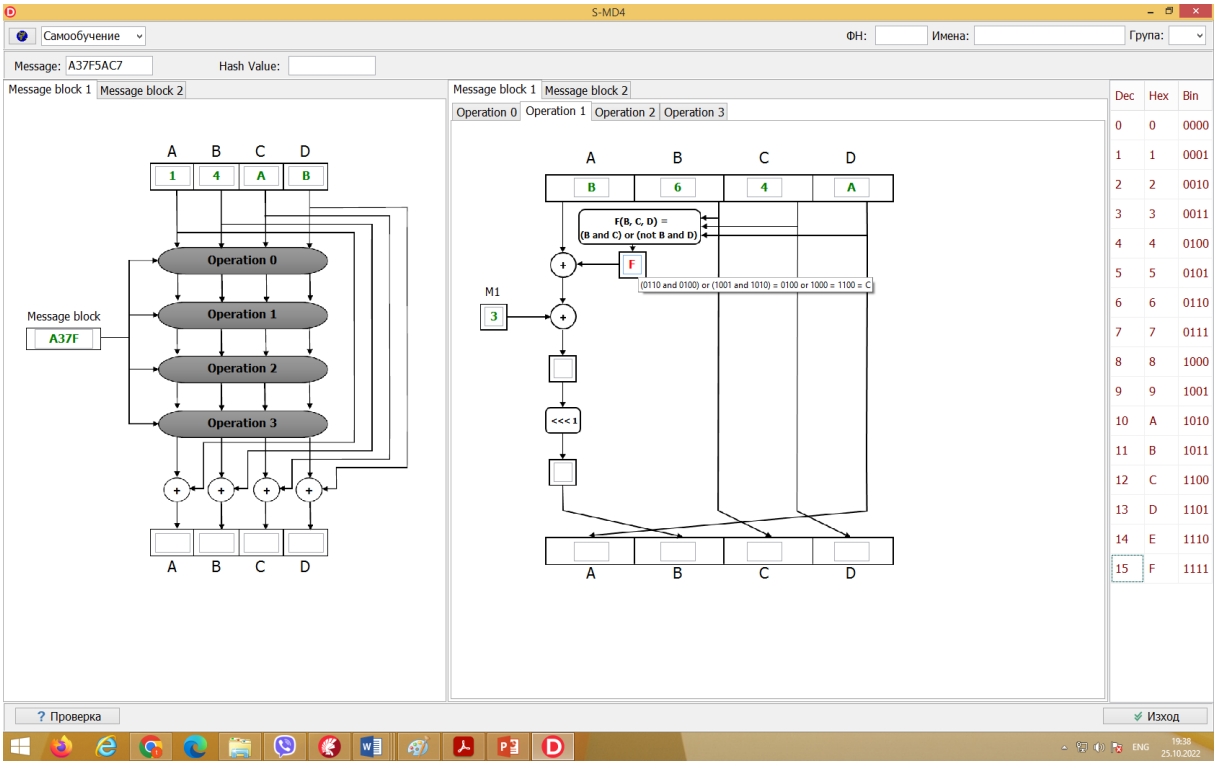
Това е режимът, при който S-MD4 Tool постъпково изпълнява алгоритъма, като автоматично попълва междинните резултати (Фиг. 2). Този режим може да се използва от преподавателя при запознаването с S-MD4. Интерфейсът на S-MD4 Tool представя алгоритъма схематично чрез два основни прозореца – за обработка на блок от съобщението и за обработка на частта от блока (M_i) в една операция. Организирането на тези обработки в отделни страници, съответно две за двата блока и четири за всяка операция от първия рунд, е удобство при необходимост от връщане назад в алгоритъма и коригиране или обяснение съдържанието на дадено поле с междинен резултат. Визуалното схематично представяне на цялостния алгоритъм, както и на отделните итерации в отделни табове подпомага разбирането на алгоритъма както и отпадането на необходимостта от използването на „лист и химикал“ за решаването на конкретни операции и запазване на междинни резултати. Предимство на обучаващото средство е и възможността за пояснява на даден резултат чрез „подсказка“ (hint), както и възможността за автоматично генериране или въвеждане на съобщение.



Фиг. 2. S-MD4 Tool в режим „Обучение“

S-MD4 Tool: Самообучение

Режимът „Самообучение“ (Фиг.3) е подобен на „Обучение“ с тази разлика, че в този режим обучаемият изпълнява постъпково алгоритъма, като попълва резултат в определени полета. Чрез бутонът „Проверка“ той може да проверява своя отговор на всяка стъпка от алгоритъма. Грешен отговор се индикира чрез оцветяването му в червено и студентът има възможност да го коригира. Функционалността на S-MD4 Tool за пояснява на очаквания резултат в поле за попълване чрез „подсказка“ (hint) също е активна.



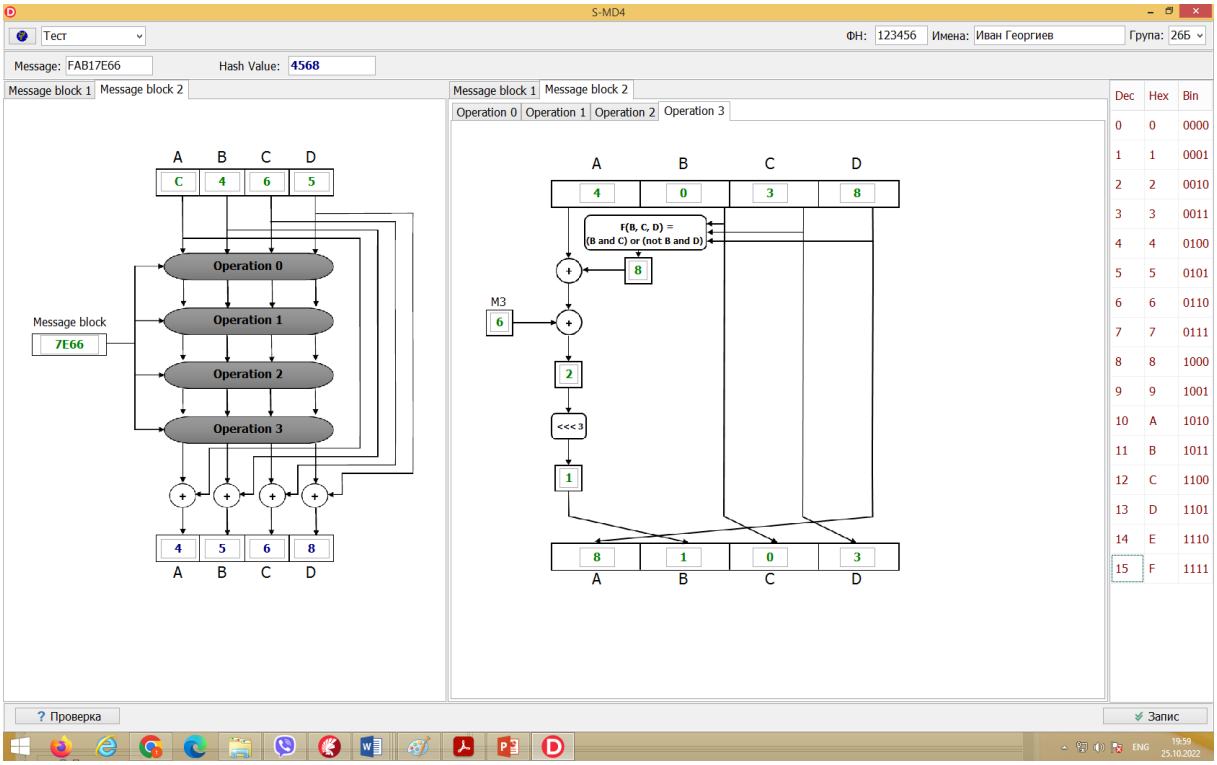
Фиг. 3. S-MD4 Tool в режим „Самообучение“

S-MD4 Tool: Тест

S-MD4 Tool може да се използва и в режим „тестване на знания“ (Фиг. 4). Разликата от режима „Самообучение“ е, че обучаемият:

- въвежда своя идентификатор (например факултетен номер) и подгрупа;
- има право само на една проверка, от която той трябва да прецени в кой момент да се възползва (след използването й, съответният бутон става неактивен);
- няма възможност за подсказка.

Резултатът от теста се пресмята автоматично като общ брой точки (който се визуализира) и се съхранява като цялостно решение във файл.



Фиг. 3. S-MD4 Tool в режим „Тест“

В условията на дистанционно обучение, където контролът върху манипулиране на резултатите от теста е занижен, е особено важно разработването на механизъм за гарантиране автентичността на крайните резултати.

Докладваният инструмент за обучение и тестване в режим на дистанционно обучение се използва от студента по подобен начин както и при присъствено обучение с тази разлика, че при генерирането на файла с резултатите, студентът има достъп до файла. За проверка целостността на информацията с резултатите от теста, S-MD4 Tool използва механизма на криптографските хеширащи функции. По този начин се S-MD4 Tool е защитен от:

- неправомерна корекция на резултатите от теста;
- решаването на няколко теста от един и същи потребител.

Разработеният софтуерен продукт може да се използва и в режим „Преподавател“ за автоматична обработка на резултатите от проведените тестове, както и за директен достъп до резултатите на даден студент. След успешна автентикация на преподавателя, той може да избере да визуализира резултатите на конкретен потребител като схема и като текстов файл или да генерира Excel – файл, обобщаващ резултатите на всички тествани.

ЗАКЛЮЧЕНИЕ

Разбирането на функционирането на MD4 е от ключово значение за разбирането на модела на съвременните криптографски функции. Използването на опростен вариант на този иначе сложен алгоритъм и имащ големи параметри – 512-битов блок на съобщението и 48 операции, разделени в 3 рунда, е подход, използван при преподаването му, който позволява детайлно разбиране на алгоритъма и „поглед отвътре“ на MD4. Използването на инструментални средства, улесняващи обучителния процес е с голямо търсене в съвременния свят.

Докладът представя подхода използван от авторите при преподаването на MD4, както и специално разработено софтуерно средство S-MD4 Tool, подпомагащо както обучаемия, така и преподавателя в различни етапи от процеса на обучение, самообучение и тестване в условия на присъствен или дистанционен учебен процес, както и автоматизирана обработка на

резултатите от тестването. Предимство на представената разработка е защитата в няколко направления на целостността на резултатите от тестването, което в условията на дистанционно обучение е особено актуален въпрос.

В заключение, опитът от практическите занятия показва, че използваният методически подход на преподаване на MD4 и на разработеното обучително средство S-MD4 Tool увеличава доброто разбиране на оригиналната пълна версия на MD4, както и на неговите наследници – алгоритмите SHA.

ACKNOWLEDGEMENTS

Този доклад се публикува с подкрепата на проект 2022–ЕЕА–01 „Анализ на алгоритми за обработка на големи масиви от данни и тяхното приложение в множество предметни области", финансиран от Фонд „Научни изследвания" на Русенски университет „Ангел Кънчев".

REFERENCES

Bosselaers, A. &. (1995). *Integrity Primitives for Secure Information Systems: Final Ripe Report of Race Integrity Primitives Evaluation (No. 1007).* Springer Science & Business Media.

Dobbertin, H. B. (1996). RIPEMD-160: A strengthened version of RIPEMD. *Fast Software Encryption. FSE 1996* (pp. 71–82). Cambridge, UK, February : Springer, Berlin, Heidelberg.

Holden, J. (2013). A Good Hash Function is Hard to Find, and Vice Versa, Cryptologia. *Cryptologia, 37*(2), 107-119.

MD4 Hash Generator. (2022). Retrieved from xhcode: https://www.xhcode.com/md4-hash-generator.html

National Institute of Standards and Technology. (1995). *Secure Hash Standard, FIPS PUB 180-1.* Washington: National Institute of Standards and Technology, U.S. Department of Commerce.

National Institute of Standards and Technology. (2001). *Secure Hash Standard, FIPS 180-2.* Washinton: National Institute of Standards and Technology.

Network Working Group. (1990, October). The MD4 Message Digest Algorithm, RFC1186. Retrieved from https://www.rfc-editor.org/rfc/rfc1186

Network Working Group. (1992, April). The MD5 Message-Digest Algorithm, RFC 1321. Retrieved from https://datatracker.ietf.org/doc/html/rfc1321

Online hash calculation MD4 Algorithm. (2022, october 17). Retrieved from conversion-tool: https://www.conversion-tool.com/md4/

Online MD4 Generator. (2022). Retrieved from Free Online File Converter: https://hash.online-convert.com/md4-generator

Online MD4 Hash Calculator. (2022, october 17). Retrieved from Md5Calc: https://md5calc.com/hash/md4